10/527820
PCT/JP2004/010432

15. 7. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

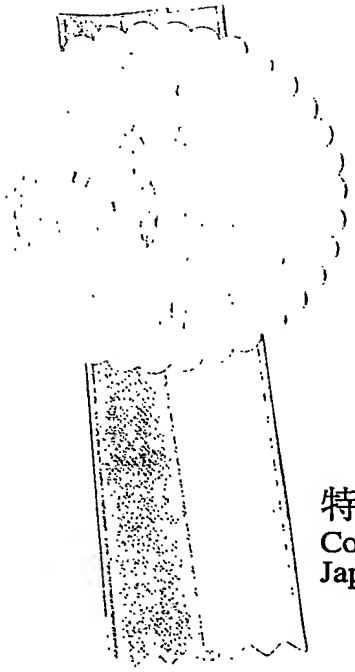
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月１６日

出願番号
Application Number: 特願２００３－２７５６７２

[ST. 10/C]: [ＪＰ２００３－２７５６７２]

出願人
Applicant(s): 松下電器産業株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　８月１９日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７４５８５

【書類名】　特許願
【整理番号】　2030750077
【提出日】　平成15年 7月16日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　高木　佳彦
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　菊地　隆文
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100105050
　【弁理士】
　【氏名又は名称】　鷲田　公一
【手数料の表示】
　【予納台帳番号】　041243
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9700376

【書類名】特許請求の範囲
【請求項１】
機器からメモリデバイスに対するアクセス方法であって、
機器にて、
メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項２】
機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項３】
機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、検証用鍵を共有化するステップと、
機器にて、
メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項４】
機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器とメモリデバイスとで、検証用鍵を共有化するステップと、
機器にて、
前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗

号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項５】
機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項６】
機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、
機器にて、
第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。
【請求項７】
機器からメモリデバイスに対するアクセス方法であって、
メモリデバイスは、
機器からのアクセスが制約された耐タンパ性の第１領域と、機器からのアクセスが制約された非耐タンパ性の第２領域と、機器からアクセスすることが可能な第３領域と、を有し、
少なくとも第１領域への処理命令である第一の処理系コマンドと、少なくとも第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、第二の処理系コマンドを用いて、第２領域へのアクセス領

域を指定する指定情報を送信するステップと、
　第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
　メモリデバイスにて、
　前記指定情報を受信するステップと、
　前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
　前記検証にて成功した場合、前記処理命令を実行するステップと、
　を有するアクセス方法。
【請求項８】
　機器からメモリデバイスに対するアクセス方法であって、
　メモリデバイスは、
　機器からのアクセスが制約された耐タンパ性の第１領域と、機器からのアクセスが制約された非耐タンパ性の第２領域と、機器からアクセスすることが可能な第３領域と、を有し、
　少なくとも第１領域への処理命令である第一の処理系コマンドと、少なくとも第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、
　機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、
　機器にて、
　第二の処理系コマンドを用いて、第２領域へのアクセス領域を指定する指定情報を送信するステップと、
　第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、
　メモリデバイスにて、
　前記指定情報を受信するステップと、
　前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
　前記検証にて成功した場合、前記処理命令を実行するステップと、
　を有するアクセス方法。

【書類名】明細書
【発明の名称】アクセス方法
【技術分野】
【０００１】
本発明は、ＰＣや携帯電話などの端末に挿入して使用されるメモリカードに対するアクセス方法に関するものである。
【背景技術】
【０００２】
従来、メモリカードは端末に挿入され、端末がデータを格納するためのものである。以下に、従来のメモリカードの一例をあげる。
【０００３】
カードは、端末から各種コマンドを受け付け、またコマンドに対するレスポンスを返すコマンド用端子（ＣＭＤライン）と、データの入力を受け付け、またデータの出力を行うデータ用端子（ＤＡＴライン）を持つ。
【０００４】
図２に示したメモリカードの例では、端子２２がＣＭＤラインとなっており、端子２７、２８、２９がＤＡＴラインであり、それぞれＤＡＴ０、ＤＡＴ１、ＤＡＴ２となっている。また端子２１はデータ入出力用とカード検出用（ＣＤ）を兼ねたＣＤ／ＤＡＴ３となっている。ＤＡＴ０～ＤＡＴ３については、ＤＡＴ０のみを使うモードと、ＤＡＴ０～３を同時に利用しＤＡＴ０のみを使う場合の４倍の転送速度を実現するモードが存在する。
【０００５】
次に、図３を用いて、従来カードのカード内モジュール構成について説明する。
【０００６】
カード内モジュールは、コントローラ３６とフラッシュメモリ３５からなる。コントローラ３６は、ＣＭＤラインに接続された、コマンド受信及びレスポンス送信を行うコマンド受信部３１と、ＤＡＴラインに接続されたデータ送受信部３２と、フラッシュメモリ３５へのデータの読み書きを行うメモリアクセス部３４と、受信したコマンドに応じてデータの読み書き処理をメモリアクセス部に要求するデータ制御部３３とからなる。
【０００７】
次に、従来のメモリカードにおける、データ読み出し時の処理動作について説明する。ここではデータの出力はＤＡＴ０端子２７のみを利用するモードに設定されているものとするが、ＤＡＴ１端子２８、ＤＡＴ２端子２９、ＤＡＴ３端子２１を併用するモードであってもよい。
【０００８】
まず、端末はカードのＣＭＤライン２２にデータ読み出しコマンドを送信する。この読み出しコマンドは図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。データ読み出しコマンドにおけるコマンド引数は、読み出し開始アドレスを格納する。
【０００９】
端末からコマンドを受信したコマンド受信部３１は、コマンドコード４０１を参照して、データ読み出しコマンドであることを認識する。
【００１０】
次に、コマンド受信部３１は、コマンド引数４０２を参照して、指定されたアドレスが正しいものであるか、つまりカードが対応している範囲に指定されたアドレスが収まっているかを調べ、アドレスが正しくなければレスポンスとしてエラーである旨のレスポンスコードを返す。アドレスが正しければ正常である旨のレスポンスコードを返す。
【００１１】
コマンド受信部３１は、レスポンスを端末に返送した後、読み出しコマンドを受信したこと及び指定アドレスをデータ制御部３３に伝える。
【００１２】

データ制御部３３は、メモリアクセス部３４に対し、コマンド受信部３１から受け取った指定アドレスとともに、読み出し要求を行う。

【００１３】

メモリアクセス部３４は、フラッシュメモリ３５の指定アドレスからデータを読み出し、データ送受信部３２に送信する。

【００１４】

データ送受信部３２は、ＤＡＴ０ライン２７を通じて、端末に読み出しデータの出力を行う。

【００１５】

このようなメモリカードでは、端末からアドレスを指定して自由にカードの読み書きが可能である。

【発明の開示】

【発明が解決しようとする課題】

【００１６】

しかし、上記のようなメモリカードにおいて、フラッシュメモリの特定領域をセキュリティ保護領域としてアクセス制限をかけ、アクセスが許可された特定の端末からのみアクセス可能としたい場合、そのコマンド引数の小ささから柔軟な認証処理を行うことができない。

【００１７】

例えば、コマンド引数にアクセス領域指定情報（アクセスするアドレスなど）と認証用の検証データを含める場合、アクセス領域に関する情報の長さが短くなればアクセス可能な領域が制限され、一方検証データの長さが短くなればセキュリティ強度が下がる。

【００１８】

一方、コマンド形態を変更すると、メモリカードへのアクセスが複雑となり、端末にとっては利用しづらいものとなる。

【００１９】

そこで本発明では、メモリカードコマンドとＩＣカードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能なアクセス方法を提供することを目的とする。

【課題を解決するための手段】

【００２０】

第１の発明は、機器からメモリデバイスに対するアクセス方法であって、機器にて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００２１】

この発明によれば、引数の小さなメモリアクセス用コマンドにおいてアクセスを許可された端末を認証することが可能となる。

【００２２】

第２の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００２３】

この発明によれば、アクセス可能な領域を柔軟に設定可能となる。

【００２４】

第３の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、検証用鍵を共有化するステップと、機器にて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００２５】

この発明によれば、アクセスのたびに検証鍵を変更することでセキュリティ強度を上げることができる。

【００２６】

第４の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器とメモリデバイスとで、検証用鍵を共有化するステップと、機器にて、前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００２７】

この発明によれば、アクセス可能な領域を柔軟に変更するとともに、アクセス可能とした領域ごとに検証用鍵を設定することができる。

【００２８】

第５の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００２９】

この発明によれば、アクセス可能な領域の共有を、メモリアクセス用コマンドとは異なるコマンド形態で行うことが可能となり、より柔軟な領域共有処理が可能となる。

【００３０】

第６の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、機器にて、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００３１】

この発明によれば、検証鍵の共有を、メモリアクセス用コマンドとは異なるコマンド形態で行うことが可能となり、より柔軟な検証鍵共有処理が可能となる。

【００３２】

第７の発明は、機器からメモリデバイスに対するアクセス方法であって、メモリデバイスは、機器からのアクセスが制約された耐タンパ性の第１領域と、機器からのアクセスが制約された非耐タンパ性の第２領域と、機器からアクセスすることが可能な第３領域と、を有し、少なくとも第１領域への処理命令である第一の処理系コマンドと、少なくとも第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、第二の処理系コマンドを用いて、第２領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００３３】

この発明によれば、端末からアクセスが制限された領域を、アクセス可能領域として共有可能となる。

【００３４】

第８の発明は、機器からメモリデバイスに対するアクセス方法であって、メモリデバイスは、機器からのアクセスが制約された耐タンパ性の第１領域と、機器からのアクセスが制約された非耐タンパ性の第２領域と、機器からアクセスすることが可能な第３領域と、を有し、少なくとも第１領域への処理命令である第一の処理系コマンドと、少なくとも第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、機器にて、第二の処理系コマンドを用いて、第２領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【００３５】

この発明によれば、端末からのアクセスが制限された領域が、カードとの間で検証用鍵を共有した端末からはアクセス可能となる。

【発明の効果】

【００３６】

本発明は、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

【発明を実施するための最良の形態】

【００３７】

本発明におけるカード内モジュール構成について図１を用いて説明する。なお、カードの端子構成は、図２に示したものと同様であるため、説明は省略する。

【００３８】

カード内モジュールは、コントローラ１０６とフラッシュメモリ１０５からなる。コントローラ１０６は、ＣＭＤラインに接続された、コマンド受信及びレスポンス送信を行う

コマンド受信部１０１と、ＤＡＴラインに接続されたデータ送受信部１０２と、フラッシュメモリ１０５へのデータの読み書きを行うメモリアクセス部１０４と、受信したコマンドに応じて、メモリアクセス部１０４、セッション鍵共有部１１０、及びパラメータ検証部１０８、暗復号部１０７に対して処理要求を行うデータ制御部１０３と、端末から受信したセキュリティ保護領域にアクセスするためのパラメータを記憶しておくパラメータ記憶部１０９と、パラメータが正しいことを検証するパラメータ検証部１０８と、端末との間で認証用及び暗復号用のセッション鍵を交換するセッション鍵共有部１１０と、セッション鍵と、セッション鍵と対応付けられたセキュリティ保護領域を記憶しておくエリア・セッション鍵管理部１１１からなる。

【００３９】

端末とセッション鍵共有部１１０との間で送受信されるコマンド形態は、一般的なＩＣカードで用いられるＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔ）フォーマットに従った形とする。つまり、セッション鍵共有部１１０はＩＣカードアプリケーションの形態をとる。

【００４０】

ここでは、ＡＰＤＵの送受信方法について説明する。

【００４１】

まず、端末からカードに対するコマンドＡＰＤＵの送信処理について説明する。

【００４２】

まず、端末はセッション鍵共有部１１０に対して送信するコマンドＡＰＤＵを作成する。次に、端末は図２のカードのＣＭＤライン２２に対して、ＡＰＤＵ送信コマンドを送信する。

【００４３】

このＡＰＤＵ送信コマンドは、従来のデータ読み出しコマンドと同様、図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

【００４４】

ＡＰＤＵ送信コマンドにおけるコマンド引数４０２は、図１４で示すように、ＤＡＴ０ラインに入力するデータがコマンドＡＰＤＵであることを示すフラグ１４０１と送信データ数を示す１４０３とからなる。フラグ１４０１及び送信データ数１４０３を合わせて３２ビットに満たない場合は未使用フィールド１４０２が存在する。

【００４５】

図２のＤＡＴ０ライン２７に入力するデータは５１２バイト単位となっており、送信データ数１４０３はこの５１２バイト単位の入力を何回行うかを示す。

【００４６】

次に、カードのコマンド受信部１０１は、端末から送信されたコマンドを受信し、それがＡＰＤＵ送信コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部１０３に対して、ＡＰＤＵ送信コマンドを受信したことを通知する。

【００４７】

次に、端末はカードのＣＭＤライン２２からＡＰＤＵ送信コマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７に図１６で示すフォーマットでコマンドＡＰＤＵ１６０２を入力する。

【００４８】

図１６において、１６０１で示される長さは後に続くＡＰＤＵ１６０２の長さを示している。長さフィールド１６０１とＡＰＤＵ１６０２の合計長にあわせてコマンド引数の送信データ数１４０３が設定されている。また、前記合計長は必ずしも５１２バイトの倍数になるわけではないので、５１２バイトの倍数になるようにパディング１６０３を付加する。

【００４９】

次に、カード内部のデータ送受信部１０２は、端末から入力されたコマンドＡＰＤＵを

受信するとともに、データ制御部１０３にコマンドＡＰＤＵを受信したことを通知する。次に、データ制御部１０３は、データ送受信部１０１からコマンドＡＰＤＵを読み出し、セッション鍵共有部１１０（ＩＣカードアプリケーション）にコマンドＡＰＤＵを渡す。

【００５０】

次に、セッション鍵共有部１１０は、コマンドＡＰＤＵに記述されたとおりの処理を行い、処理の結果生じたデータとステータス情報をレスポンスＡＰＤＵとしてデータ制御部１０３に渡す。

【００５１】

次に、カードから端末に対するレスポンスＡＰＤＵの送信処理について説明する。

【００５２】

ここでは、前記のコマンドＡＰＤＵの送信方法で示したとおり、セッション鍵共有部１１０が出力したレスポンスＡＰＤＵがデータ制御部１０３で保持されている状態であるものとする。

【００５３】

まず、端末は、カードのＣＭＤライン２２に対して、ＡＰＤＵ受信コマンドを送信する。このＡＰＤＵ受信コマンドは、ＡＰＤＵ送信コマンドと同様、図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。ＡＰＤＵ受信コマンドにおけるコマンド引数４０２は、図１５で示すように、送信データ数を示す１５０２とからなる。送信データ数１５０２が３２ビットに満たない場合は未使用フィールド１５０１が存在する。

【００５４】

図２のＤＡＴ０２７から出力されるデータは、ＡＰＤＵ送信コマンドにおける入力データと同様に５１２バイト単位となっており、送信データ数１５０２は５１２バイト単位で何回出力を行うかを示す。

【００５５】

次に、カードのコマンド受信部１０１は、端末から送信されたコマンドを受信し、それがＡＰＤＵ受信コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部１０３に対して、ＡＰＤＵ受信コマンドを受信したことを通知する。

【００５６】

次に、データ制御部１０３は、データ送受信部１０２に対して、セッション鍵共有部１１０から受け取ったレスポンスＡＰＤＵを渡す。

【００５７】

次に、端末は、カードのＣＭＤライン２２からＡＰＤＵ受信コマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７からレスポンスＡＰＤＵを読み出す。読み出されるレスポンスＡＰＤＵは、図１６で示すフォーマットで出力される。各フィールドの詳細については、ＡＰＤＵ送信コマンドにおける入力時と同様であるため、説明を省略する。

【００５８】

カードに搭載されるフラッシュメモリ１０５は、図６に示すように、少なくとも端末から従来の読み出し用コマンド及び書き込み用コマンドでアクセスすることが可能な通常領域６２と、前記の従来のコマンドではアクセスすることができないセキュリティ保護領域６１を持つ。

【００５９】

セキュリティ保護領域６１は、通常、カードアプリケーションからのみアクセス可能な状態であって、端末からの従来の読み出し用コマンド及び書き込み用コマンドに対しては、コマンド受信部１０１によってアクセスは排除される。

【００６０】

本発明におけるメモリカードは内部に複数のカードアプリケーションを搭載することが可能となっており、図７のように、セキュリティ保護領域６１は各アプリケーションに対して個別の領域（ＡＰ１用領域７１～ＡＰ３用領域７３）が割り当てられる。

【００６１】

セキュリティ保護領域６１は、データ制御部１０３が管理する格納用暗号鍵で暗号化されている。この暗号鍵は、セキュリティ保護領域６１全体で１つのＫｓであってもよいし、各アプリケーション用のＡＰ１用領域７１～ＡＰ３用領域７３に個別にＫｓ＿１～Ｋｓ＿３を用意してもよい。本実施の形態では各アプリケーションＡＰ１～３に格納用暗号鍵Ｋｓ＿１～Ｋｓ＿３を用意する。

【００６２】

次に、セキュリティ保護領域６１内の各アプリケーション用のＡＰ１用領域７１～ＡＰ３用領域７３の内部構成について、図８を用いて説明する。

【００６３】

ここでは、例としてカードアプリケーションＡＰ１用領域７１をあげている。ＡＰ１用領域７１の内部はディレクトリＤＩＲ１，ＤＩＲ２とファイルＦＩＬＥ１～ＦＩＬＥ３を用いた階層構造を用いたデータ管理となっている。

【００６４】

カードアプリケーションＡＰ１は、ＡＰ１用領域７１内でディレクトリ移動を行い、目的のファイルが存在するディレクトリＤＩＲ１，ＤＩＲ２上でファイルＦＩＬＥ１～ＦＩＬＥ３に対する読み書きを行う。

【００６５】

例えば、カードアプリケーションＡＰ１がファイルＦＩＬＥ３にアクセスする場合は、ディレクトリＤＩＲ１に移動し、次にディレクトリＤＩＲ２に移動した後、ファイルＦＩＬＥ３の読み書きを行う。また、各ディレクトリＤＩＲ１，ＤＩＲ２において、その下位のディレクトリまたはファイルの作成及び削除が可能である。

【００６６】

次に、カード内のセッション鍵共有部１１０と、端末との間で行われるセッション鍵共有手順について図９～図１２を用いて説明する。

【００６７】

カードアプリケーションと端末はそれぞれ公開鍵暗号で用いられる公開鍵と秘密鍵の対を保持し、お互いに相手の公開鍵を保持している。

【００６８】

セッション鍵共有手順におけるコマンド形態は前記で示したＡＰＤＵを用いる。以降の説明においてはコマンド形態に関する記述を行わず、単にコマンド、レスポンスと表記する。

【００６９】

まず、端末は、ＳＥＬＥＣＴコマンドを送信することで、カードアプリケーションＡＰ１の選択を行う（ステップ９０１）。

【００７０】

カードは、端末から指定されたカードアプリケーションＡＰ１の選択が正常に完了すれば正常完了のレスポンス、完了しなければ異常終了のレスポンスを返す（ステップ９０２）。

【００７１】

次に、端末は、処理９０３を実行する。この処理９０３の詳細については、図１０のフローチャートを参照して説明する。

【００７２】

端末は、乱数Ｒｈの生成を行い（ステップＳ９０３１）、乱数Ｒｈと、端末がアクセスしたい図８で示したファイルＦＩＬＥ３のファイル名を結合し、カードアプリケーションＡＰ１が保持する秘密鍵ＰｒｉＳに対応した公開鍵ＰｕｂＳで暗号化してＤＡＴＡ１を生成し（ステップＳ９０３２）、さらに端末が保持する秘密鍵ＰｒｉＨに対応した公開鍵ＰｕｂＨを示す識別子Ｉｎｆｏ＿ＰｕｂＨとＤＡＴＡ１を結合してＤＡＴＡ２を生成する（ステップＳ９０３３）。

【００７３】

図９に戻り、次に、端末は、カードアプリケーションとのセッション鍵の共有及び、端

末がアクセス可能な領域情報の共有を行うために、ステップＳ９０３３で生成したＤＡＴＡ２を含んだＲＥＱ＿ＡＲＥＡ＿ＩＮＦＯコマンドをカードアプリケーションに送信する（ステップ９０４）。

【００７４】

ＲＥＱ＿ＡＲＥＡ＿ＩＮＦＯコマンドを受信したカードアプリケーションＡＰ１は、処理９０５を実行する。この処理９０５の詳細については、図１１のフローチャートを参照して説明する。

【００７５】

カードアプリケーションＡＰ１は、ＤＡＴＡ２よりＤＡＴＡ１を抽出し、カードアプリケーションＡＰ１が保持する秘密鍵ＰｒｉＳで復号化し、乱数ＲｈとファイルＦＩＬＥ３を得る（ステップＳ９０５１）。

【００７６】

次に、ＤＡＴＡ２より公開鍵を識別して識別子Ｉｎｆｏ＿ＰｕｂＨを抽出し、Ｉｎｆｏ＿ＰｕｂＨが示す公開鍵ＰｕｂＨに対応付けられた端末がファイルＦＩＬＥ３にアクセスする権限があるかを確認する。権限がなければ、その旨のエラーをレスポンスとして端末に返す。アクセスする権限があれば、ＦＩＬＥ３のファイルサイズＳＩＺＥ３を取得する（ステップＳ９０５２）。

【００７７】

次に、乱数Ｒｓを生成し（ステップＳ９０５３）、ファイルＦＩＬＥ３を端末からアクセス可能となるように設定を行い、端末がアクセスするときに使用するためのエリア番号Ｘをファイル ＦＩＬＥ３に割り当て、ファイルサイズＳＩＺＥ３とともにエリア・セッション鍵管理部１１１に記憶する（ステップＳ９０５４）。

【００７８】

次に、乱数Ｒｓ、エリア番号Ｘ、ファイルサイズＳＩＺＥ３を結合し、ＤＡＴＡ３を生成し（ステップＳ９０５５）、ＤＡＴＡ３を端末の公開鍵ＰｕｂＨで暗号化してＤＡＴＡ４を生成する（ステップＳ９０５６）。

【００７９】

次に、乱数Ｒｓと乱数Ｒｈに排他的論理和を施し、乱数Ｒを生成し（ステップＳ９０５７）、乱数Ｒから暗号用セッション鍵Ｋｄ、検証用セッション鍵Ｋｍを生成する（ステップＳ９０５８）。

【００８０】

次に、セッション鍵Ｋｄ及びＫｍをエリア番号Ｘと関連付け、エリア・セッション鍵管理部１１１に記憶する（ステップＳ９０５９）。

【００８１】

図９に戻り、カードはここまでの処理を終えると端末にＤＡＴＡ４を含んだレスポンスＡＰＤＵを端末に送信する（ステップ９０６）。

【００８２】

レスポンスＡＰＤＵを受信した端末は、処理９０７を実行する。この処理９０７の詳細については、図１２のフローチャートを参照して説明する。

【００８３】

端末は、端末の秘密鍵ＰｒｉＨを用いてＤＡＴＡ４を復号しＤＡＴＡ３を取得する（ステップＳ９０７１）。次に、端末は、ＤＡＴＡ３より乱数Ｒｓを取得し、乱数Ｒｓと乱数Ｒｈに排他的論理和を施し、乱数Ｒを生成し（ステップＳ９０７２）、乱数Ｒから暗号用セッション鍵Ｋｄ、検証用セッション鍵Ｋｍを生成する（ステップＳ９０７３）。

【００８４】

以上のステップ９０１から９０７を踏むことで、端末とカード間の相互認証を行い、かつ端末が指定したファイルに対するアクセス権限があれば端末からのアクセスが可能な状態となり、またアクセスする際に必要なエリア番号、エリア番号に割り当てられたファイルのサイズ、および検証用セッション鍵、暗号用セッション鍵を共有することができる。

【００８５】

なお、ステップ９０４において端末からカードに伝えられるファイル名は、カードアプリケーションが管理するファイルを直接示すものである必要はなく、カードアプリケーションがどのファイルを指しているかが認識できる形であればよい。

【００８６】

また、端末がアクセスしたいファイル及びステップＳ９０５４において、そのファイルに対して端末がアクセス可能となる設定を行った際に割り当てられるエリア番号が常に同じとなるようにし、これらの情報を端末とカード間であらかじめ認識しておくことで、ステップ９０４における端末がアクセスしたいファイル名の通知およびステップ９０６におけるファイルに割り当てられたエリア番号の通知を省略することもできる。

【００８７】

さらに、本説明では、各カードアプリケーションが図８で示すようにディレクトリとファイルからなる階層構造をもち、ディレクトリ名およびファイル名でデータを管理している形態で説明したが、カードアプリケーションに割り当てられた領域を適当な大きさに分割し、分割されたそれぞれの領域に番号のような識別子を割り当てて管理する形態でもよい。その場合は、図９で示した処理手順で用いられるファイル名ＦＩＬＥ３の代わりに前記識別子を用いる。

【００８８】

次に、端末からセキュリティ保護領域に対してアクセスを行う際の処理について図１３及び図１を用いて説明する。

【００８９】

まず、端末はカードに対してアクセス領域指定コマンドを送信する（ステップ１３０１）。このアクセス領域指定コマンドは、ＡＰＤＵ送信コマンドと同様、図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

【００９０】

アクセス領域指定コマンドにおけるコマンド引数４０２は、図１４で示すように、ＤＡＴ０ライン２７に入力するデータがアクセス領域指定情報であることを示すフラグ１４０１と送信データ数を示す１４０３とからなる。フラグ１４０１及び送信データ数１４０３を合わせて３２ビットに満たない場合は未使用フィールド１４０２が存在する。

【００９１】

ＤＡＴ０ライン２７に入力するデータは、５１２バイト単位となっており、送信データ数１４０３は、この５１２バイト単位の入力を何回行うかを示す。

【００９２】

次に、カードのコマンド受信部１０１は、端末から送信されたコマンドを受信し、それがアクセス領域指定コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部１０３に対して、アクセス領域指定コマンドを受信したことを通知する（ステップ１３０２）。

【００９３】

次に、端末はカードのＣＭＤライン２２からアクセス領域指定コマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７に図１７で示すフォーマットでアクセス領域指定情報１７０２を入力する（ステップ１３０３）。

【００９４】

図１７の１７０１で示される長さは、後に続くアクセス領域指定情報１７０２の長さを示している。長さフィールド１７０１とアクセス領域指定情報１７０２の合計長に合わせてコマンド引数４０２の送信データ数１４０３が設定されている。また、前記合計長は必ずしも５１２バイトの倍数になるわけではないので、５１２バイトの倍数になるようにパディング１７０３を付加する。

【００９５】

アクセス領域指定情報１７０２は、図１８で示されるように、図９のステップ９０６でカードから通知されたエリア番号Ｘを指定するエリア番号１８０１と、０～同じくカード

から通知されたファイルサイズＳＩＺＥ３の範囲で選択可能なアクセス開始アドレス１８０２と、１～（ファイルサイズＳＩＺＥ３－アクセス開始アドレス１８０２）の範囲で選択可能なアクセスデータサイズ１８０３とで構成される。

【００９６】

次に、カード内部のデータ送受信部１０２は、端末から入力されたアクセス領域指定情報１７０２を受信するとともに、データ制御部１０３にアクセス領域指定情報１７０２を受信したことを通知する。

【００９７】

次に、データ制御部１０３は、データ送受信部１０２からアクセス領域指定情報１７０２を読み出し、エリア番号１８０１が、図１１のステップＳ９０５４にて割り当てられたエリア番号Ｘであるか、アクセス開始アドレス及びアクセスデータサイズは、エリア番号Ｘと対応したファイルのファイルサイズ範囲に収まっているかをチェックし、異常があればエラーフラグを設定する。

【００９８】

データ制御部１０３は、異常がなければ、図１に示すパラメータ記憶部１０９にアクセス領域指定情報１７０２を記憶する。

【００９９】

以上が、アクセス領域を指定する処理である。

【０１００】

次に、図６のセキュリティ保護領域６１に対して読み出しを行う際の処理について説明する。

【０１０１】

図１３において、端末は、カードに対してセキュリティ保護領域読み出しコマンドを送信する（ステップ１３０４）。このセキュリティ保護領域読み出しコマンドは、ＡＰＤＵ送信コマンドと同様、図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

【０１０２】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数４０２は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末と同一であるか、またセッション鍵共有手順を経てエリア番号Ｘが示す領域に対するアクセス権限があることを確認された端末と同一であるかを検証するための検証データからなる。

【０１０３】

この検証データの生成方法について図５を用いて説明する。

【０１０４】

アクセス領域指定情報１７０２は、アクセス領域指定コマンドにおいてＤＡＴラインに入力するパラメータである。検証鍵５０１は、図９のステップ９０７で生成した検証用セッション鍵Ｋｍである。

【０１０５】

検証データ作成部５０３は、暗号演算を行うモジュールである。ここでは、ＤＥＳ－ＭＡＣと呼ばれるＭＡＣ生成処理を行う。アクセス領域指定情報１７０２に対してパディングデータ５０５を付加した５０２を入力データとして、検証鍵５０１を用いてＤＥＳ暗号を用いたＭＡＣ生成処理を行い、検証データとしてＭＡＣデータ５０４を作成する。

【０１０６】

パディングデータ５０５については、端末からカードに対してアクセス領域指定コマンドを送信するときにアクセス領域指定情報１７０２と併せて送信してもよいし、あらかじめ端末とカードの間で取り決めをしたパディング生成ルールに基づいて生成したパディングデータを付与してもよい。

【０１０７】

なお、本実施の形態ではＤＥＳ－ＭＡＣを用いて検証データを作成しているが、他のア

ルゴリズムを用いてもよい。

【０１０８】

なお、端末が正当であるか認証する必要がなく、アクセス領域指定コマンドとの対応付けのみ確認したい場合は、暗号処理を用いずに、単にＳＨＡ１やＭＤ５アルゴリズムを用いたハッシュデータを検証データとして用いてもよい。

【０１０９】

端末は、上記の検証データ生成処理によって３２ビットの検証データを生成し、セキュリティ保護領域読み出しコマンドの引数として使用する。

【０１１０】

次に、カードのコマンド受信部１０１は、端末から送信されたコマンドを受信し、それがセキュリティ保護領域読み出しコマンドであることを認識し、アクセス領域指定情報１７０２に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。また、アクセス領域指定情報１７０２に関するエラーフラグが設定されていない場合は、図１３で示すように、端末に正常レスポンスを返す（ステップ１３０５）とともに、データ制御部１０３に対してセキュリティ保護領域読み出しコマンドを受信したことを通知し、パラメータ検証部１０８にコマンド引数４０２として与えられた検証データ５０４を渡す。

【０１１１】

次に、端末は、カードのＣＭＤライン２２からセキュリティ保護領域読み出しコマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７からデータが出力されるのを待つ。

【０１１２】

以降にカードによるセキュリティ保護領域のデータ出力処理について説明する。

【０１１３】

カードのパラメータ検証部１０８は、パラメータ記憶部１０９からアクセス領域指定コマンドによって端末から与えられ、記憶しておいたアクセス領域指定情報１７０２を読み出し、アクセス領域指定情報１７０２に含まれるエリア番号Ｘ（１８０１）に対応する、図１１のステップＳ９０５９で記憶した検証用セッション鍵Ｋｍをエリア・セッション鍵管理部１１１から取得する。

【０１１４】

次に、カードのパラメータ検証部１０８は、検証用セッション鍵Ｋｍとアクセス領域指定情報１７０２を用いて、図１９に示した検証データ生成処理を行い、検証データ１９０４を生成する。なお、検証データ生成処理については、図５で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

【０１１５】

次に、カードのパラメータ検証部１０８は、上記検証データ生成処理で生成した検証データ１９０４と、端末からセキュリティ保護領域読み出しコマンドの引数によって与えられた検証データ５０４を比較し、一致しなければエラーとし、データ読み出し処理に移行しない。一致した場合は、次のデータ読み出し処理に移行することをデータ制御部１０３に通知する。

【０１１６】

次に、カードのデータ制御部１０３は、パラメータ記憶部１０９からアクセス領域指定情報１７０２を読み出し、その中に含まれるエリア番号Ｘを取得し、エリア・セッション鍵管理部１１１からエリア番号に対応するファイルＦＩＬＥ３を認識する。

【０１１７】

次に、カードのデータ制御部１０３は、ファイルＦＩＬＥ３がアプリケーションＡＰ１用の領域であることを確認し、格納用暗号鍵Ｋｓ＿１を取得する。

【０１１８】

次に、カードのデータ制御部１０３は、アクセス領域指定情報１７０２からアクセス開始アドレス１８０２とアクセスデータサイズ１８０３を取得し、ファイルＦＩＬＥ３として管理されている領域に対して、アクセス開始アドレス１８０２をオフセット、アクセス

データサイズ１８０３を読み出しサイズとしてメモリアクセス部１０４にデータ読み出し要求を行う。

【０１１９】

次に、カードのデータ制御部１０３は、暗復号部１０７に対して、メモリアクセス部１０４によって読み出されたデータを格納用暗号鍵Ｋｓ＿１で復号化するよう要求する。

【０１２０】

次に、カードのデータ制御部１０３は、暗復号部１０７に対して、暗復号部１０７によって復号化されたデータを暗号用セッション鍵Ｋｄで暗号化するよう要求する。

【０１２１】

次に、カードのデータ制御部１０３は、データ送受信部１０２に対して、暗復号部１０７によって暗号用セッション鍵Ｋｄで暗号化されたデータを端末に送信するよう要求する。

【０１２２】

上記の処理によって、カードからセキュリティ保護領域のデータがセッション鍵Ｋｄによって暗号化された状態で出力可能となる。

【０１２３】

端末は、カードからデータが出力可能となったことを認識し、図１３に示すように、ＤＡＴ０ライン２７からセッション鍵Ｋｄによって暗号化された状態のデータを取得し（ステップ１３０６）、端末が保持する暗号用セッション鍵Ｋｄによってデータを復号化し、アクセス領域指定情報１７０２で指定した領域のデータを得る。

【０１２４】

次に、セキュリティ保護領域に対して書き込みを行う際の処理について、図２０を参照して説明する。

【０１２５】

端末は、カードに対してセキュリティ保護領域書き込みコマンドを送信する（ステップ２００４）。このセキュリティ保護領域書き込みコマンドは、ＡＰＤＵ送信コマンドと同様、図４で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

【０１２６】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数４０２は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末と同一であるか、またセッション鍵共有手順を経てエリア番号Ｘが示す領域に対するアクセス権限があることを確認された端末と同一であるかを検証するための検証データ１９０４からなる。

【０１２７】

この検証データの生成方法についてはセキュリティ保護領域読み出しコマンドと同様であるため、詳細な説明は省略する。

【０１２８】

端末は、検証データ生成処理によって３２ビットの検証データを生成し、セキュリティ保護領域書き込みコマンドの引数として使用する。

【０１２９】

次に、カードのコマンド受信部１０１は、端末から送信されたコマンドを受信し、それがセキュリティ保護領域書き込みコマンドであることを認識し、アクセス領域指定情報１７０２に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。

【０１３０】

また、アクセス領域指定情報１７０２に関するエラーフラグが設定されていない場合は、端末に正常レスポンスを返す（ステップ２００５）とともに、データ制御部１０３に対してセキュリティ保護領域書き込みコマンドを受信したことを通知し、パラメータ検証部１０８にコマンド引数として与えられた検証データ５０４を渡す。

【０１３１】

次に、端末は、カードのＣＭＤライン２２からセキュリティ保護領域書き込みコマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７にデータの入力を行う（ステップ２００６）。ここでＤＡＴ０ライン２７に入力するデータは、図９のステップ９０７で生成した暗号用セッション鍵Ｋｄで暗号化したものである。また、入力データサイズは、アクセス領域指定情報１７０２で指定したアクセスデータサイズと同一である。

【０１３２】

以降にカードによるセキュリティ保護領域へのデータ格納処理について説明する。

【０１３３】

カードのパラメータ検証部１０８は、パラメータ記憶部１０９からアクセス領域指定コマンドによって端末から与えられ、記憶しておいたアクセス領域指定情報１７０２を読み出し、アクセス領域指定情報１７０２に含まれるエリア番号Ｘ（１８０１）に対応する、図１１のステップ９０５９で記憶した検証用セッション鍵Ｋｍをエリア・セッション鍵管理部１１１から取得する。

【０１３４】

次に、カードのパラメータ検証部１０８は、検証用セッション鍵Ｋｍとアクセス領域指定情報１７０２を用いて、図１９に示した検証データ生成処理を行い、検証データ１９０４を生成する。なお、検証データ生成処理については、図５で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

【０１３５】

次に、カードのパラメータ検証部１０８は、上記で生成した検証データ１９０４と、端末からセキュリティ保護領域書き込みコマンドの引数によって与えられた検証データ５０４を比較し、一致しなければエラーとし、データ書き込み処理に移行しない。一致した場合は次のデータ書き込み処理に移行することをデータ制御部１０３に通知する。

【０１３６】

次に、カードのデータ制御部１０３は、パラメータ記憶部１０９からアクセス領域指定情報１７０２を読み出し、その中に含まれるエリア番号Ｘを取得し、エリア・セッション鍵管理部１１１からエリア番号に対応するファイルＦＩＬＥ３を認識する。

【０１３７】

次に、カードのデータ送受信部１０２は、端末から入力されたデータを受信する。

【０１３８】

次に、カードのデータ制御部１０３は、ファイルＦＩＬＥ３がアプリケーションＡＰ１用の領域であることを確認し、格納用暗号鍵Ｋｓ＿１を取得する。

【０１３９】

次に、カードのデータ制御部１０３は、暗復号部１０７に対して、データ送受信部１０２が受信したデータを暗号用セッション鍵Ｋｄで復号化するよう要求する。

【０１４０】

次に、カードのデータ制御部１０３は、暗復号部１０７に対して、暗復号部１０７が復号化したデータを格納用暗号鍵Ｋｓ＿１で暗号化するよう要求する。

【０１４１】

次に、カードのデータ制御部１０３は、アクセス領域指定情報１７０２からアクセス開始アドレス１８０２とアクセスデータサイズ１８０３を取得し、ファイルＦＩＬＥ３として管理されている領域に対し、アクセス開始アドレス１８０２をオフセット、アクセスデータサイズ１８０３を書き込みサイズとして、メモリアクセス部１０４に対してデータ書き込み要求を行う。

【０１４２】

上記のようにして、端末が入力したセッション鍵Ｋｄで暗号化されたデータを格納鍵Ｋｓ＿１で暗号化してフラッシュメモリに格納する。

【０１４３】

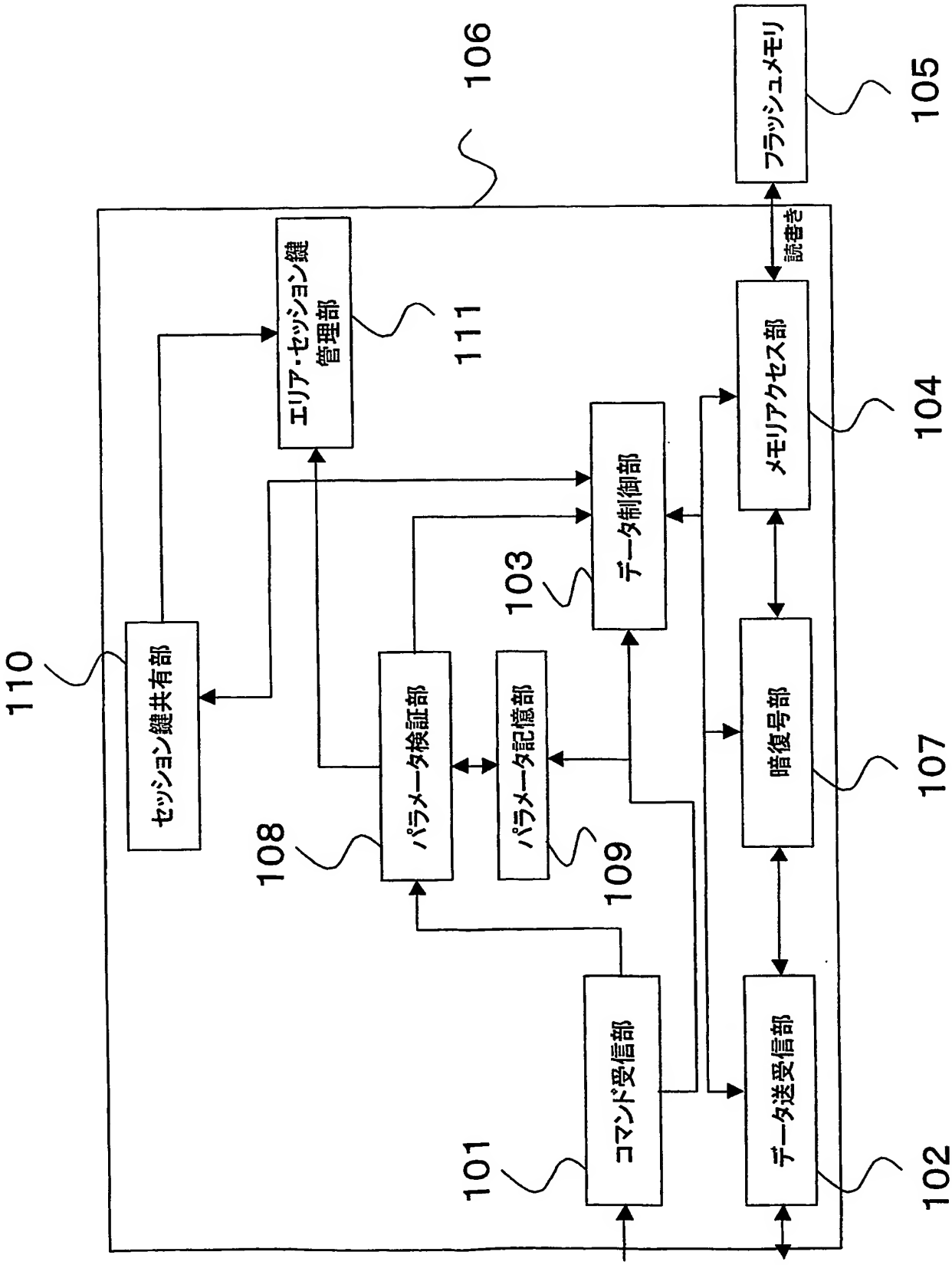
本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を１つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

【０１４４】
本実施の形態では、図９にてセッション鍵共有手順を含めているが、セキュリティポリシーとしてセッション鍵を毎回更新する必要がないと考える場合は、端末およびカードがあらかじめ検証鍵および暗号鍵を保持し、それをセッション鍵として用いてもよい。
【０１４５】
以上、本発明のように、ＩＣカード用コマンドとメモリアクセス用コマンドを受信可能なメモリカードにおいて、カードアプリケーションが利用し、通常はカードアプリケーション経由でのみアクセス可能であり、端末からのアクセスが制限されているセキュリティ保護領域に対して、カードアプリケーションと端末が相互認証し、カードアプリケーションがアクセス可能設定を行うことにより、端末からメモリアクセス用コマンドを用いてアクセスすることが可能となる。
【０１４６】
また、カードアプリケーションがアクセス可能設定を行うためのカードアプリケーションと端末間の相互認証は、用途が限定されたメモリアクセス用コマンドではなく、ＩＣカード用コマンドを使うことにより、データのセキュリティレベルに応じて相互認証方式を柔軟に選択可能となる。
【０１４７】
また、メモリアクセス用コマンドに含められる引数サイズが３２ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。
【０１４８】
また、検証用及び暗号用セッション鍵の共有処理をセキュリティ保護領域アクセスのたびに行うことにより、セキュリティ保護領域アクセスに含める検証データとして適当な値を設定して繰り返し不正アクセスを行う攻撃に対する防御性を高めることができる。
【０１４９】
また、端末からアクセスしたいファイルをカードに通知し、それにエリア番号を割り当て、カードから端末に通知することにより、端末がアクセス可能な領域を設定することが可能となる。また、複数のファイルに対して行うことにより、同時に複数のファイルに対してアクセス可能な状態を作ることができる。
【産業上の利用可能性】
【０１５０】
本発明にかかるアクセス方法は、メモリカードコマンドとＩＣカードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能とすることである。
【図面の簡単な説明】
【０１５１】
【図１】本発明の一実施の形態におけるメモリカードの内部モジュール構成を示す図
【図２】カードの端子を示す図
【図３】従来のメモリカードの内部モジュール構成を示す図
【図４】本実施の形態におけるメモリカードのコマンドフォーマットを示す図
【図５】本実施の形態における端末の正当性検証を行うための検証データの端末による生成方法を示す図
【図６】本実施の形態におけるフラッシュメモリの内部構成を示す図
【図７】本実施の形態におけるセキュリティ保護領域の内部構成を示す図
【図８】本実施の形態におけるセキュリティ保護領域内の各アプリケーション用領域の内部構成を示す図
【図９】本実施の形態におけるセッション鍵共有及びアクセス可能領域共有手順を示

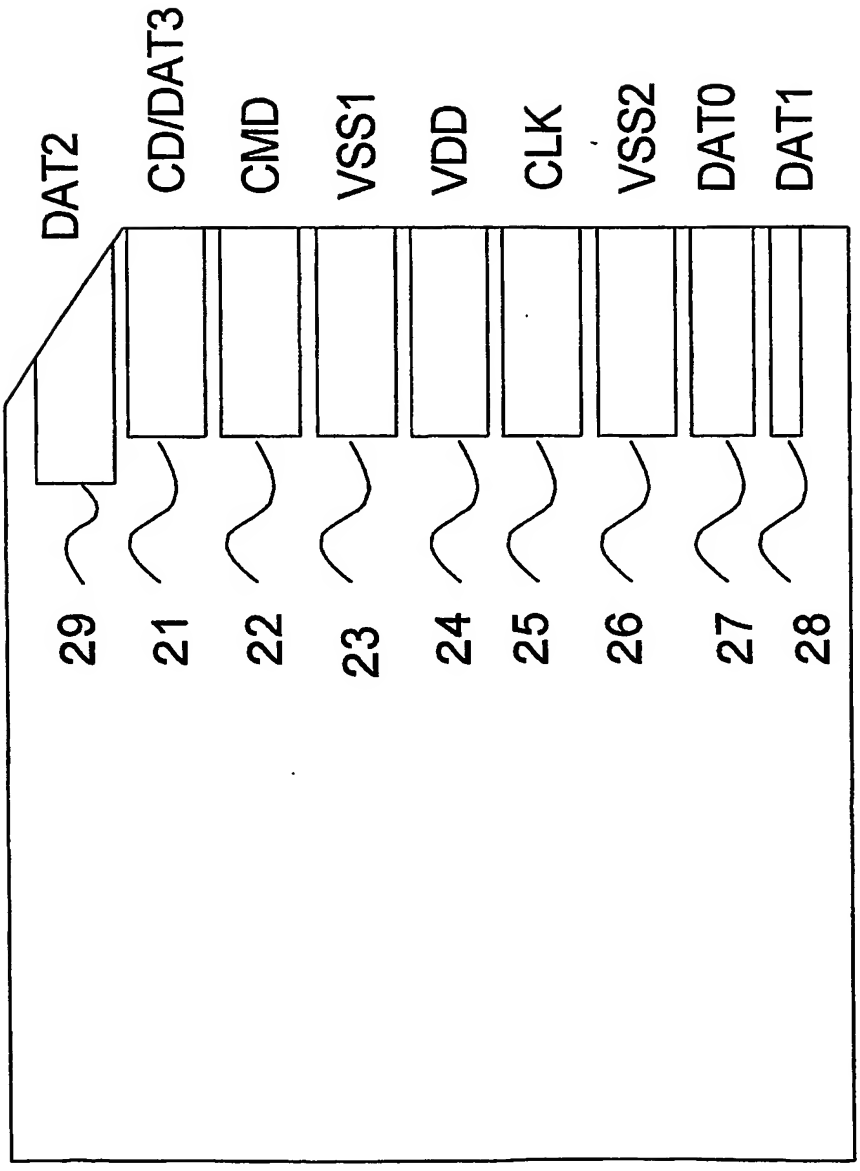
す図
【図１０】図９のステップ９０３における処理の詳細を説明するためのフローチャート
【図１１】図９のステップ９０５における処理の詳細を説明するためのフローチャート
【図１２】図９のステップ９０７における処理の詳細を説明するためのフローチャート
【図１３】本実施の形態における端末からセキュリティ保護領域を読み出すためのコマンドシーケンスを示す図
【図１４】本実施の形態におけるＡＰＤＵ送信コマンドの引数フォーマットを示す図
【図１５】本実施の形態におけるＡＰＤＵ受信コマンドの引数フォーマットを示す図
【図１６】本実施の形態におけるＡＰＤＵ送信コマンドの入力データ及びＡＰＤＵ受信コマンドの出力データのフォーマットを示す図
【図１７】本実施の形態におけるアクセス領域指定コマンドの入力データフォーマットを示す図
【図１８】本実施の形態におけるアクセス領域指定情報を示す図
【図１９】本実施の形態における端末の正当性検証を行うための検証データのカードによる生成方法を示す図
【図２０】本実施の形態における端末からセキュリティ保護領域に書き込むためのコマンドシーケンスを示す図

【符号の説明】
【０１５２】
１０１　コマンド受信部
１０２　データ送受信部
１０３　データ制御部
１０４　メモリアクセス部
１０５　フラッシュメモリ
１０６　コントローラ
１０７　暗復号部
１０８　パラメータ検証部
１０９　パラメータ記憶部
１１０　セッション鍵共有部
１１１　エリア・セッション鍵管理部

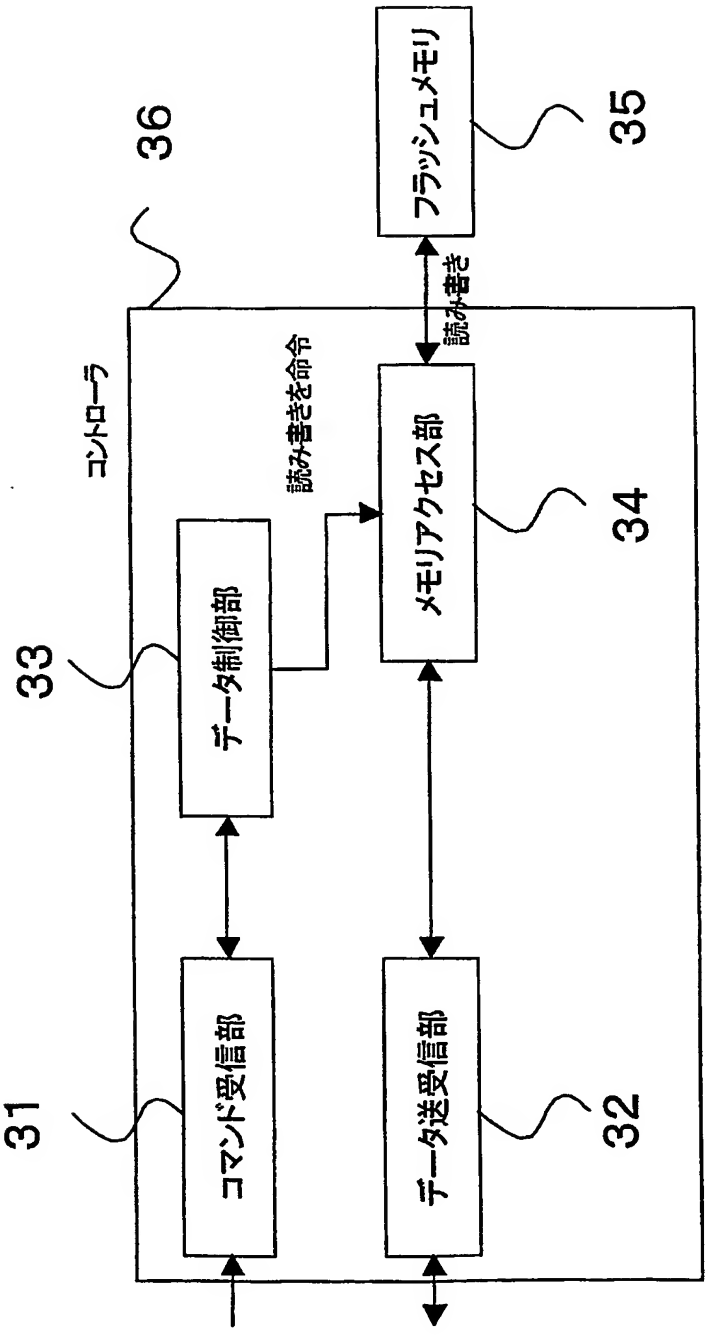
【書類名】図面
【図１】


106
フラッシュメモリ
105
エリア・セッション鍵
管理部
111
読書き
メモリアクセス部
104
データ制御部
103
セッション鍵共有部
110
パラメータ検証部
108
パラメータ記憶部
109
暗復号部
107
コマンド受信部
101
データ送受信部
102

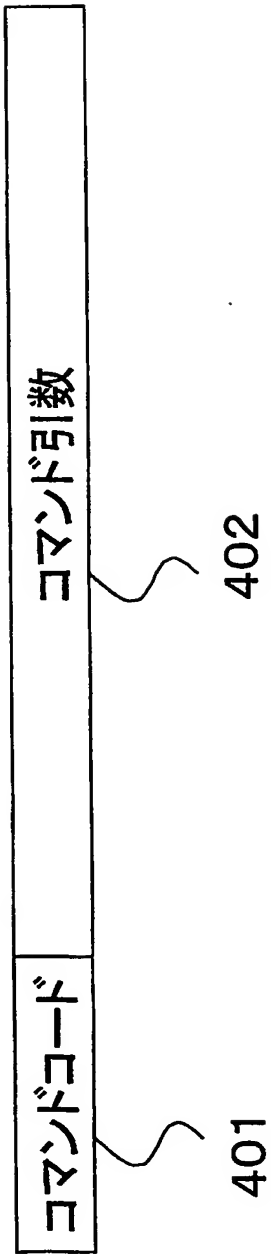
【図２】


DAT2
CD/DAT3
CMD
VSS1
VDD
CLK
VSS2
DAT0
DAT1
29
21
22
23
24
25
26
27
28

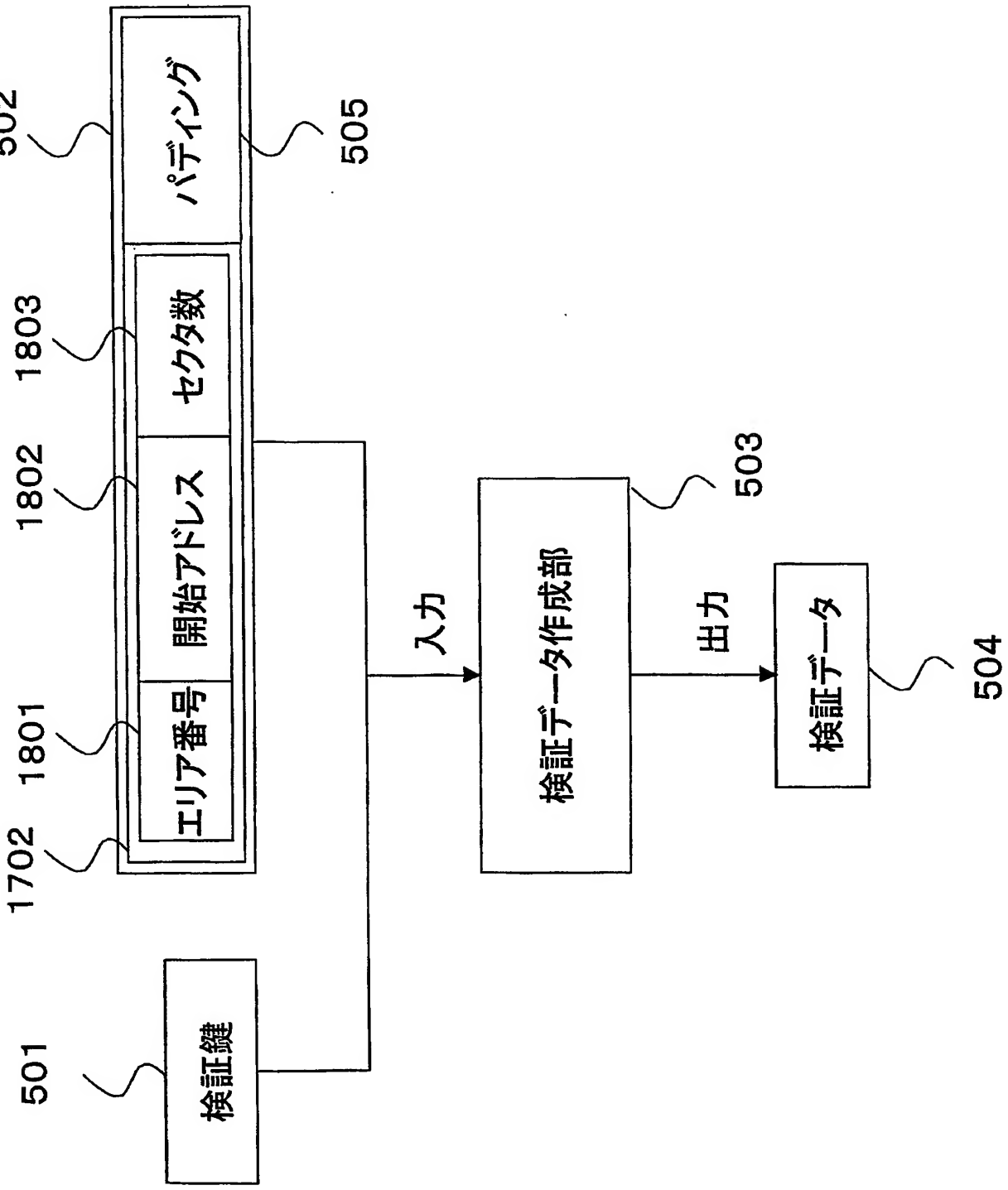
【図３】


フラッシュメモリ
35
36
読み書き
コントローラ
読み書きを命令
メモリアクセス部
34
データ制御部
33
コマンド受信部
31
データ送受信部
32

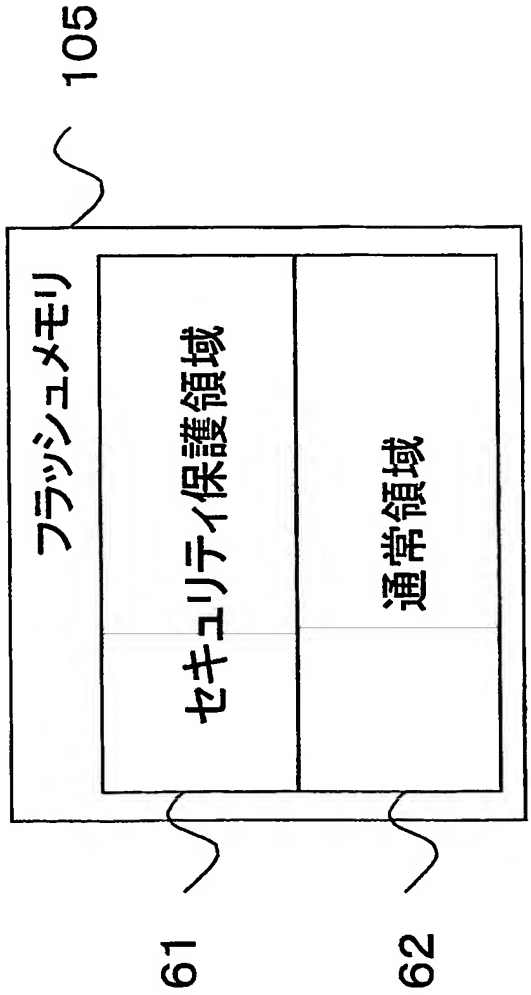
【図４】



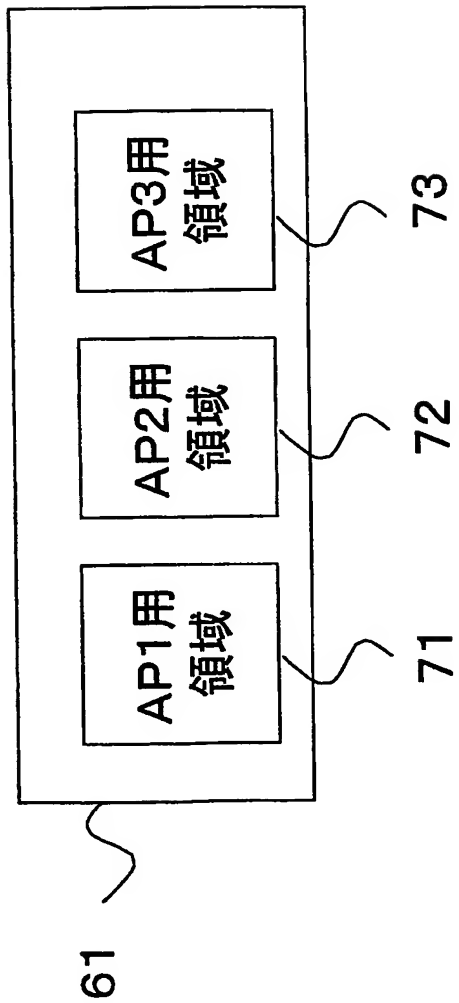
【図５】


502
505
パディング
1803
セクタ数
1802
開始アドレス
1801
エリア番号
1702
501
検証鍵
入力
検証データ作成部
503
出力
検証データ
504

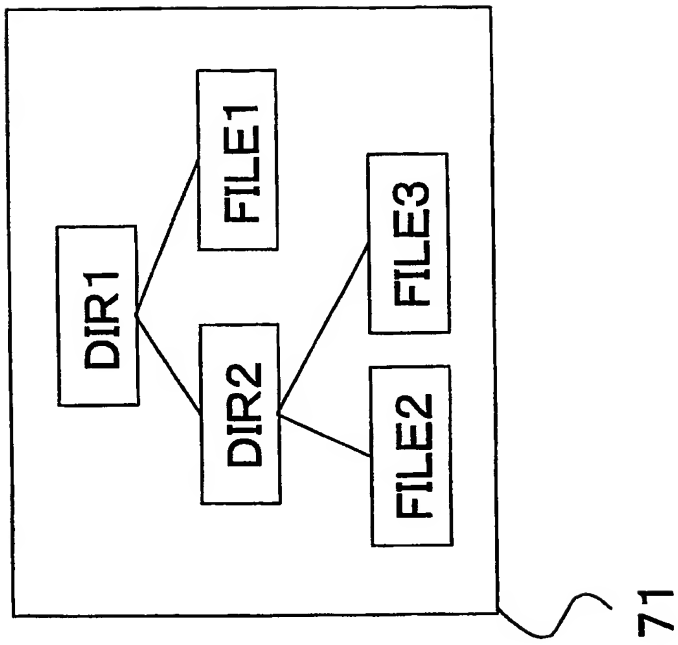
【図６】



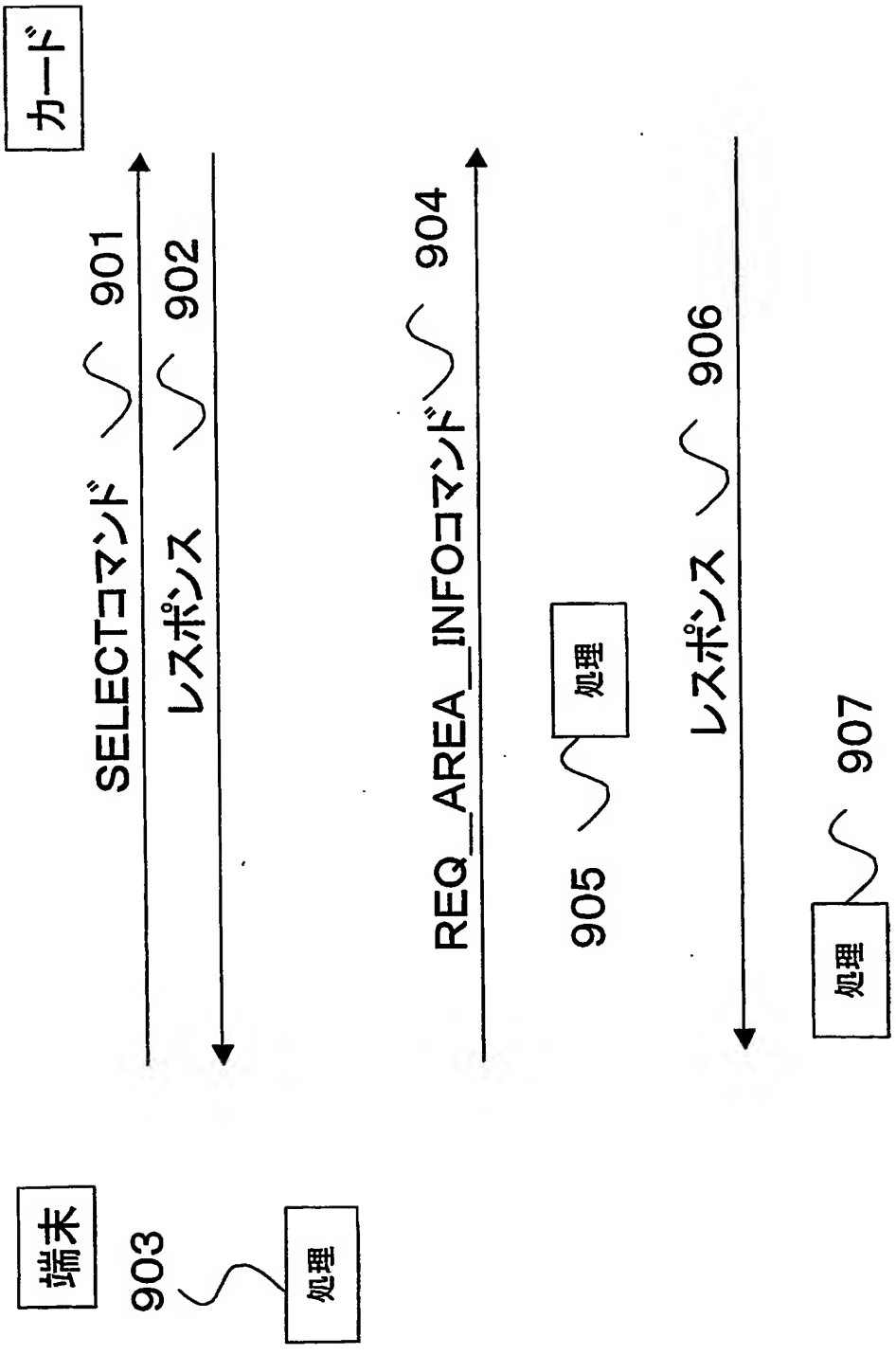
【図７】



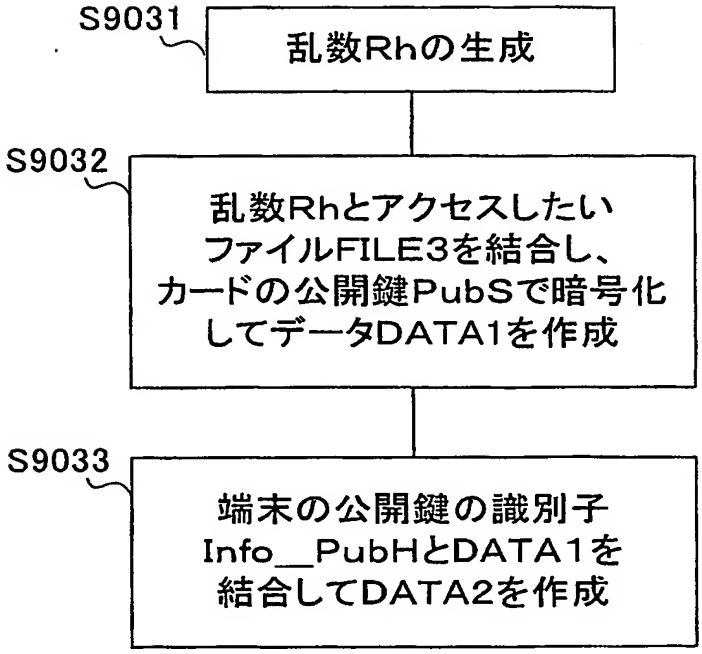
【図８】



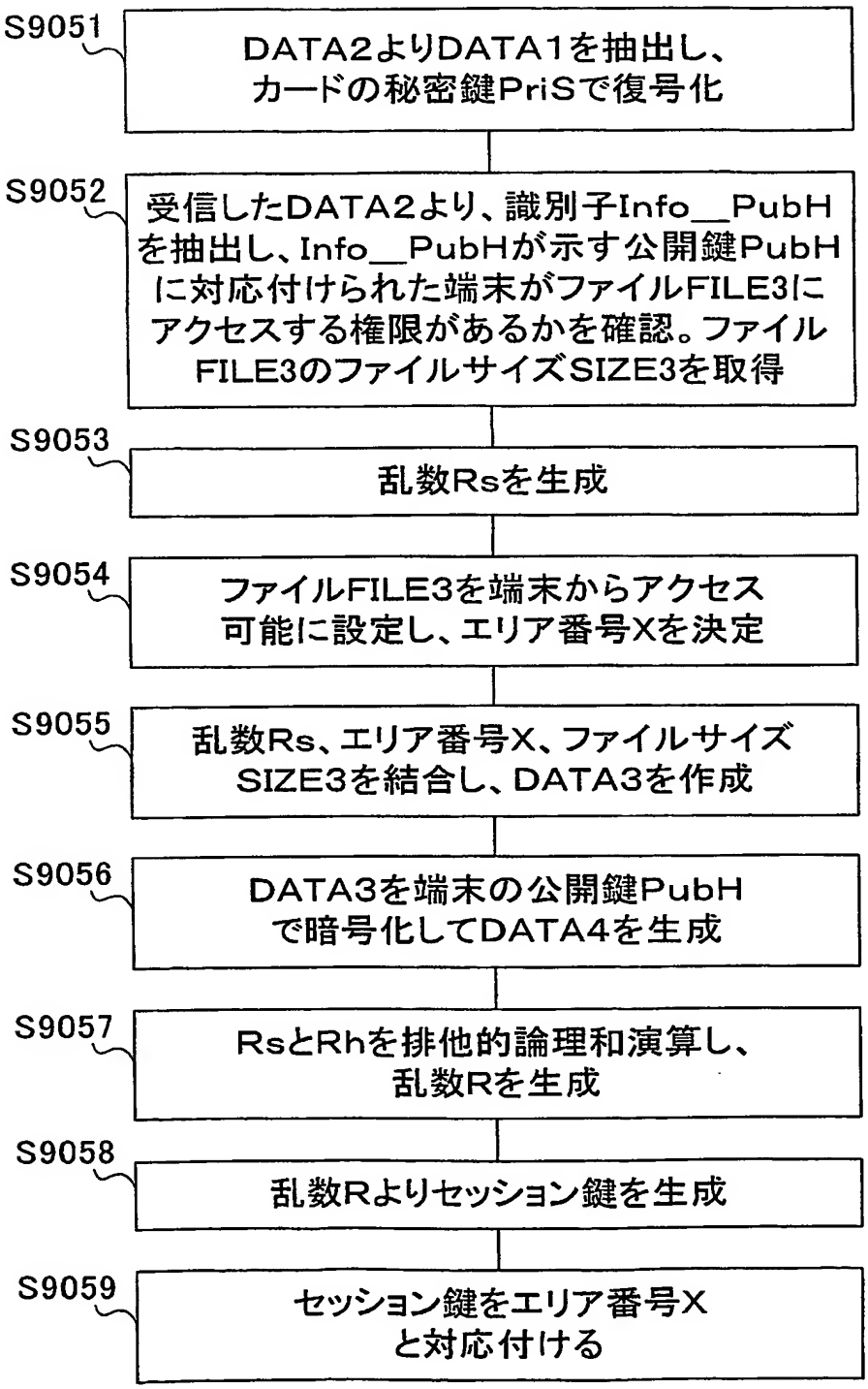
【図９】


カード
SELECTコマンド
901
レスポンス
902
REQ_AREA_INFOコマンド
904
処理
905
レスポンス
906
処理
907
端末
903
処理

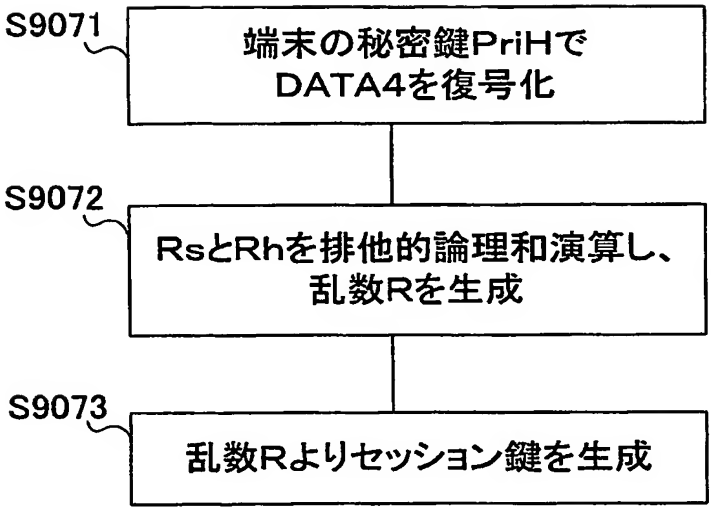
【図１０】


S9031
乱数Rhの生成
S9032
乱数Rhとアクセスしたい
ファイルFILE3を結合し、
カードの公開鍵PubSで暗号化
してデータDATA1を作成
S9033
端末の公開鍵の識別子
Info_PubHとDATA1を
結合してDATA2を作成

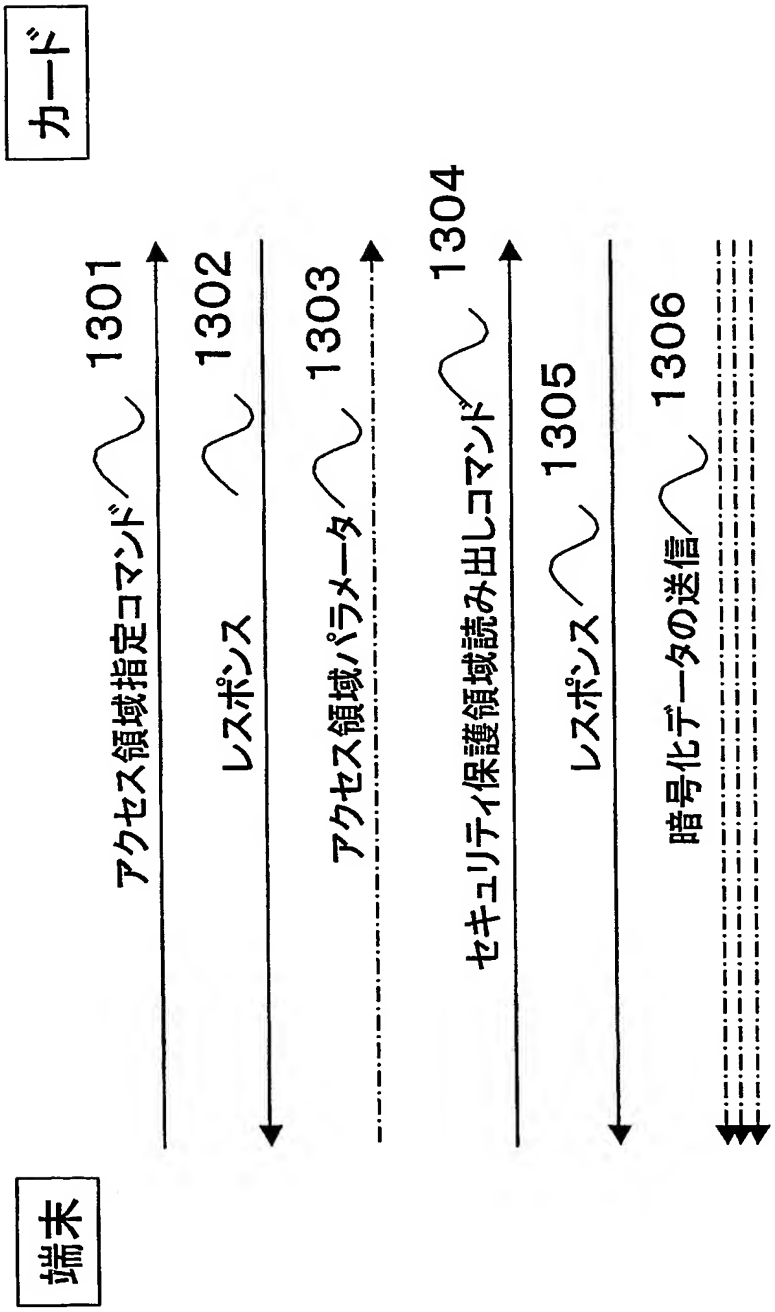
【図１１】


S9051
DATA2よりDATA1を抽出し、
カードの秘密鍵PriSで復号化
S9052
受信したDATA2より、識別子Info__PubH
を抽出し、Info__PubHが示す公開鍵PubH
に対応付けられた端末がファイルFILE3に
アクセスする権限があるかを確認。ファイル
FILE3のファイルサイズSIZE3を取得
S9053
乱数Rsを生成
S9054
ファイルFILE3を端末からアクセス
可能に設定し、エリア番号Xを決定
S9055
乱数Rs、エリア番号X、ファイルサイズ
SIZE3を結合し、DATA3を作成
S9056
DATA3を端末の公開鍵PubH
で暗号化してDATA4を生成
S9057
RsとRhを排他的論理和演算し、
乱数Rを生成
S9058
乱数Rよりセッション鍵を生成
S9059
セッション鍵をエリア番号X
と対応付ける

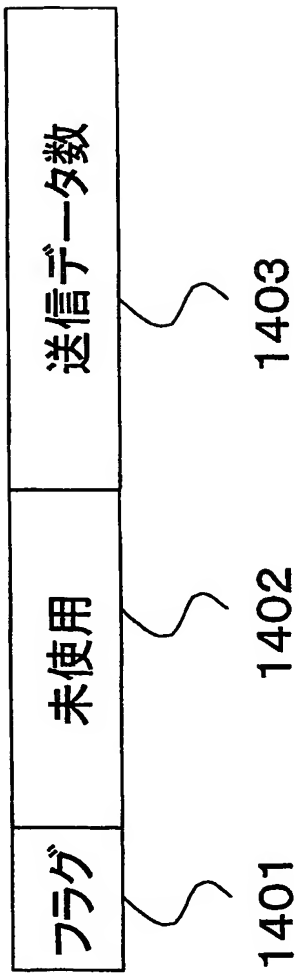
【図１２】


S9071
端末の秘密鍵PriHで
DATA4を復号化
S9072
RsとRhを排他的論理和演算し、
乱数Rを生成
S9073
乱数Rよりセッション鍵を生成

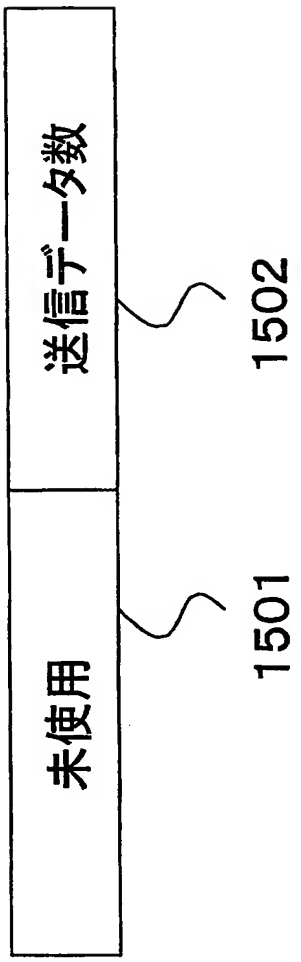
【図１３】


カード
端末
アクセス領域指定コマンド
1301
レスポンス
1302
アクセス領域パラメータ
1303
セキュリティ保護領域読み出しコマンド
1304
レスポンス
1305
暗号化データの送信
1306

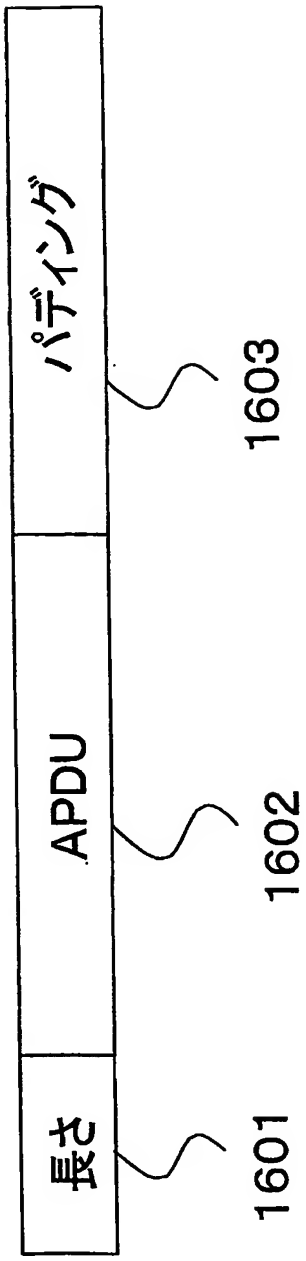
【図１４】



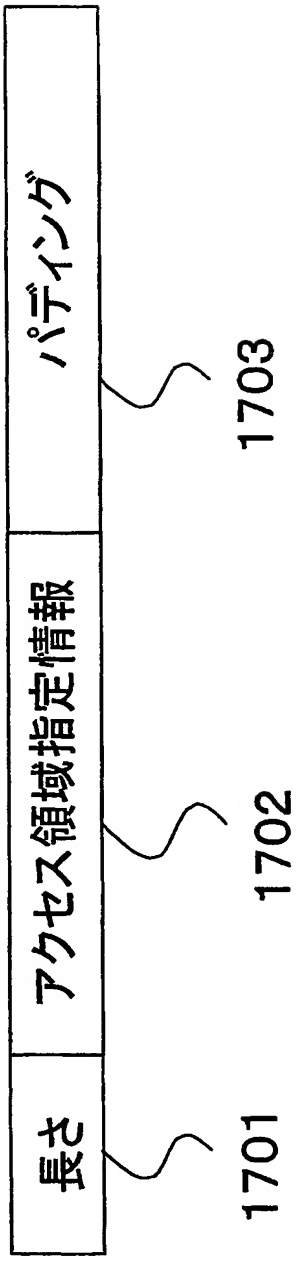
【図１５】



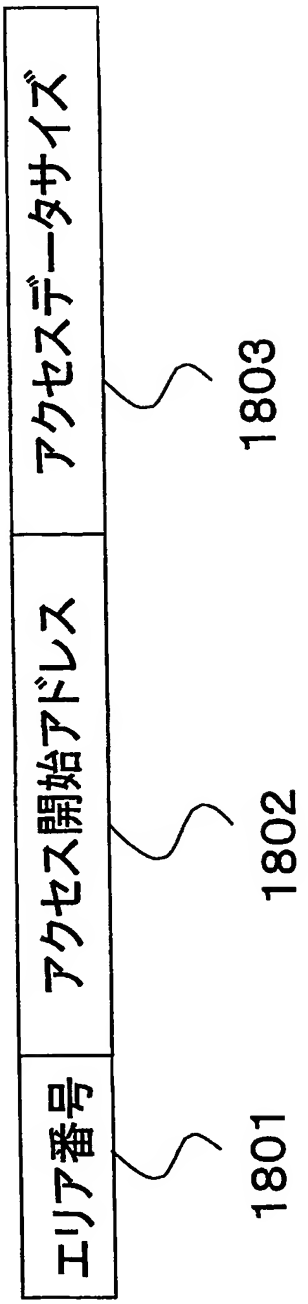
【図１６】



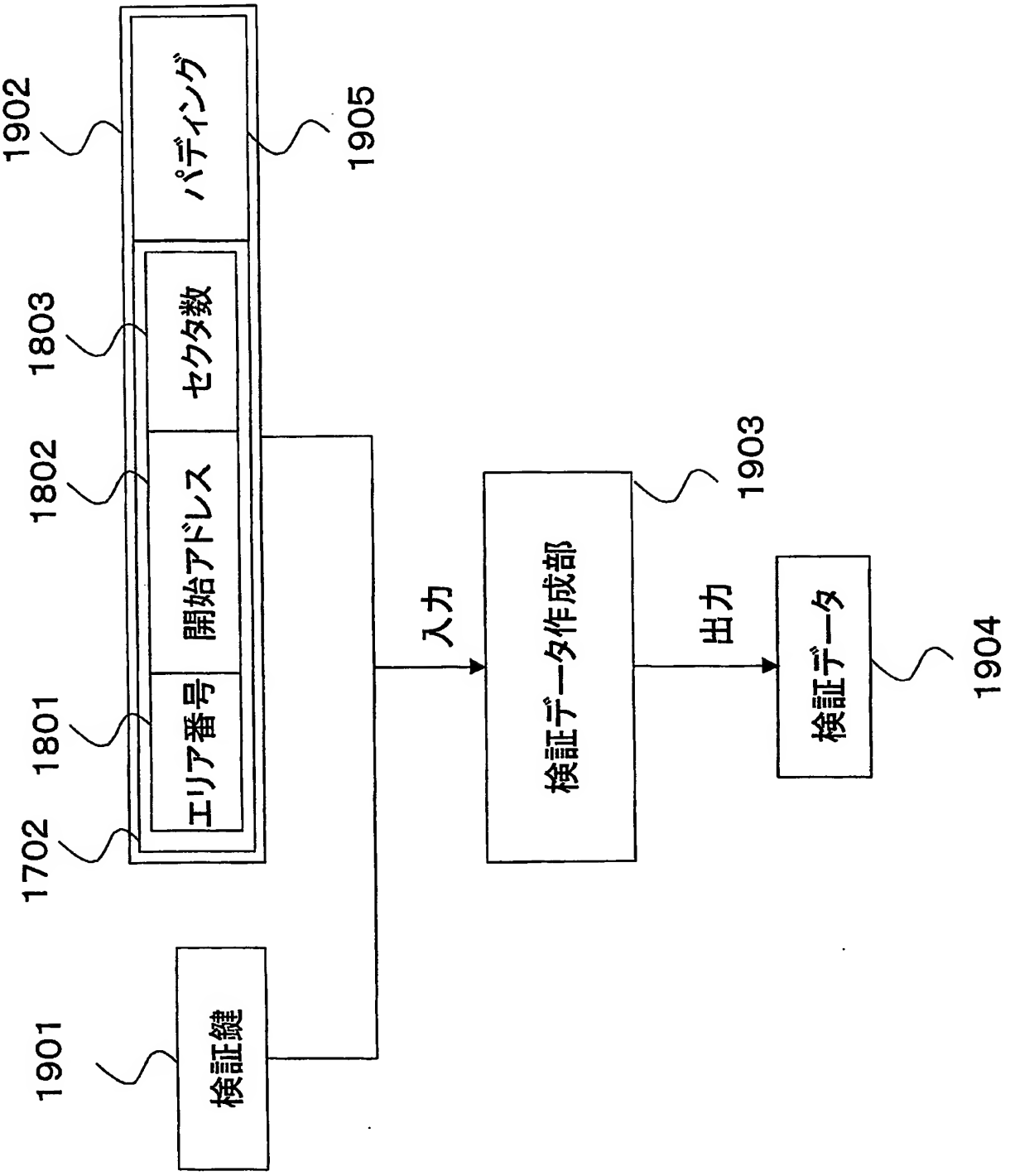
【図１７】



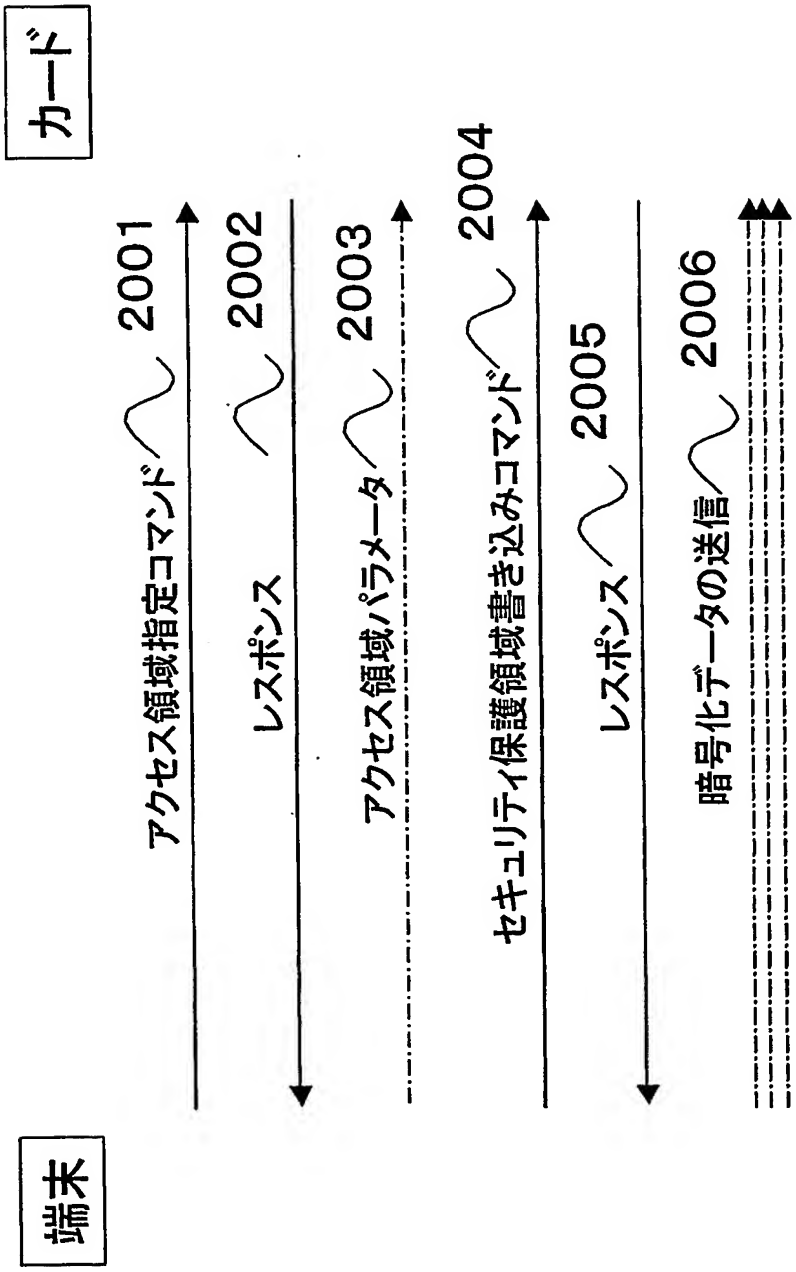
【図１８】



【図１９】


1902
パディング
1905
1803
セクタ数
1802
開始アドレス
1801
エリア番号
1702
1901
検証鍵
入力
1903
検証データ作成部
出力
検証データ
1904

【図２０】


カード
端末
アクセス領域指定コマンド
2001
レスポンス
2002
アクセス領域パラメータ
2003
セキュリティ保護領域書き込みコマンド
2004
レスポンス
2005
暗号化データの送信
2006

【書類名】要約書

【要約】

【課題】　コマンド引数の小さいメモリカードコマンドにおいて、アクセス権限をもった端末を安全に認証可能とする。

【解決手段】　端末からアクセス領域を指定するコマンドと、アクセスを行うコマンドを分離し、アクセスを行うコマンドの引数に端末の検証データを含めて送信することで、アクセス領域を指定するコマンドを発行した端末アプリケーションとアクセスを行うコマンドを発酵した端末アプリケーションと、検証用鍵を保有する端末アプリケーションが同一であることが検証可能となる。

【選択図】　図１

特願２００３－２７５６７２

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社